REMARKS

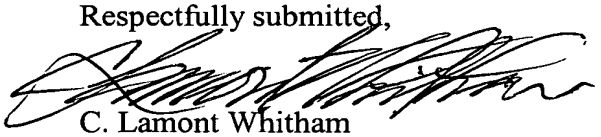
The undersigned wishes to thank the Examiner, Mr. Benjamin E. Lanier, and his Supervisory Primary Examiner, Mr. Giberto Barron, for the courtesies shown to him and one of the co-inventors, Mr. Matthew Kamerman, at a personal interview on September 14, 2005. An agreement was reached at the interview to file this amendment to claim 80 together with a Request for Continued Examination (RCE). The Messrs. Lanier and Barron suggested the amendment and indicated that the amendment would eliminate the patent to Gennaro et al. as a reference; however, since the amendment raised new issues, it was agreed that the amendment would be presented as a preliminary amendment with the RCE.

At the interview, Messrs. Lanier and Barron were presented with a document that included a side-by-side analysis of the claimed invention and the patent to Gennaro et al. along with flow charts diagraming each of claims 80 and 81. Mr. Kamerman provided a description of the origin of the invention and how it is being implemented. It was agreed at the interview that the side-by-side analysis would be made of record and, therefore, a copy is attached as an exhibit.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 80 and 81 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

Respectfully submitted,



C. Lamont Whitham
Reg. No. 22,424

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190
Tel. (703) 787-9400
Fax. (703) 787-7557
Customer No.: 30743

FIELD OF TECHNOLOGY

Claimed Invention	Gennaro et al.
Customizing browsing experience of a user of a Web site, such as a healthcare Web site, which includes the user's and others' medical histories while maintaining the privacy and security of the user as well as those whose medical histories are contained in the Web site.	System for verifying the identity of an individual in a way that provides enhanced identity verification security using encryption and biometric techniques in order to authorize the individual to access a database or resource.

PROBLEM SOLVED

Claimed Invention	Gennaro et al.
Categorizing and quantifying the personal information of a user in a way that will enable the determination of Web pages that are likely to be of interest to the user, particularly as it relates to a user's medical problem and where the possession of the necessary data is made problematic by privacy and security mandates; e.g., by the HIPAA statute regarding the possession and processing of medical data.	Providing a secure, two-factor authentication method to identify and authenticate users of an information database or other secured resource, while not requiring that users keep a physical authentication token in their possession. Further, protecting from theft the biometric reading or model used to provide the second authentication factor.

STRUCTURE

Claimed Invention	Gennaro et al.
Each user is assigned a unique Universal Anonymous Identifier (UAI) which is generated by a third party registration authority, is encrypted by the registration authority under a key unknown to the Web site operator, and then provided to the Web site operator. The Web site operator correlates and indexes the de-identified medical data by the encrypted UAI, or by an alternative key assigned by the Web site operator and mapped by the operator to the encrypted UAI. The database contains de-identified medical data of the user and others. Access to the database is a process of obtaining a Personal Identifier (PID) from the user to determine a first anonymous identifier (the UAI), using the first anonymous identifier to access a first database to authenticate the user, determining a second anonymous identifier (the encrypted UAI) which is used to access the database containing the de-identified medical data.	Enrollment of an individual is by means of a biometric sample, a password, and a personal identifier. The biometric sample or a biometric model derived from the sample is encrypted using a key derived from the password, and placed in an authentication database indexed by the personal identifier. Authorization to access to an information database is gained by inputting the personal identifier, password and a biometric sample. The personal identifier is used to access the encrypted biometric sample or model that was stored on enrollment, and the password is used to decrypt the stored biometric sample or model, which is statistically compared with the newly input biometric sample are statistically compared. If the comparison exceeds a threshold, the individual is authorized to access to the information database.

FUNCTION

Claimed Invention	Gennaro et al.
Based on a user's medical code history, the user's browsing experience is customized by, for example, Web pages having medical codes similar to the user's medical code history suggested to the user, automatically modifying searches conducted by the user to search for Web pages relating to the medical code history of the user, and/or Web pages may be suggested to the user based on Web pages visited by users with similar medical code histories. These functions are accomplished without revealing the user's identity or the identity of others whose medical records are in the database. Moreover, inspection of the medical records in the database can not reveal the identities of those to whom the records pertain.	The biometric information stored in a secure manner is used to verify the identity of an individual and authorize access to the information database or other secured resource.

ADVANTAGES

Claimed Invention	Gennaro et al.
A user is provided with access to a database while protecting the privacy of the user. In addition, the information in the database, such as a medical records database, is de-identified so as to protect the privacy of the those whose medical records are contained in the database. The user's personal information (e.g., medical history) is used to customize the user's Web browsing experience.	An individual seeking access to an informational database or other secured resource is identified and positively authenticated using biometric information. The biometric information provided during enrollment has been encrypted so as to better maintain the security of the authentication database, whereas prior biometric authentication methods have left their biometric databases vulnerable to theft.

GENERAL COMMENTS

The work that gave rise to claimed invention relates to Web searches of medical records which, because of the very nature of the subject matter to be searched, requires strict privacy of the users whose medical records are searched. However, personal information about the user, i.e., medical history, is used in order to customize searches for the user so as to produce more meaningful and relevant information for the user. This is much more powerful an aid to searching than, for example, a history of prior searches made by the user or, for that matter, prior searches made by others relating to the same subject matter. The invention, in effect, de-identifies the user from his or her personal information. Moreover, the information searched is de-identified so that the personal information of others in the database cannot be associated them.

Having developed the invention for the specific application of searching medical records, the inventors realized that the invention has broader application than searching medical records. In a society which is more and more exposed to invasion of privacy, the invention can provide a valuable search tool for those who wish to remain anonymous in their inquiries. The claims which are currently pending are not, therefore, limited to the searching of medical records *per se*, although the information accessed is "personal information, associated with a plurality of users". The search that is done by a user is anonymous and the personal information of other users is also anonymous.

CLAIMS CURRENTLY PENDING

Claim 80. A method of accessing personal information, associated with a plurality of users and stored in a computer system, in a manner that protects the privacy of users, wherein each user has a personal identifier and a plurality of anonymous identifiers, comprising the steps of:

prompting a user for the user's personal identifier;

determining a first anonymous identifier from information derived from the user's personal identifier;

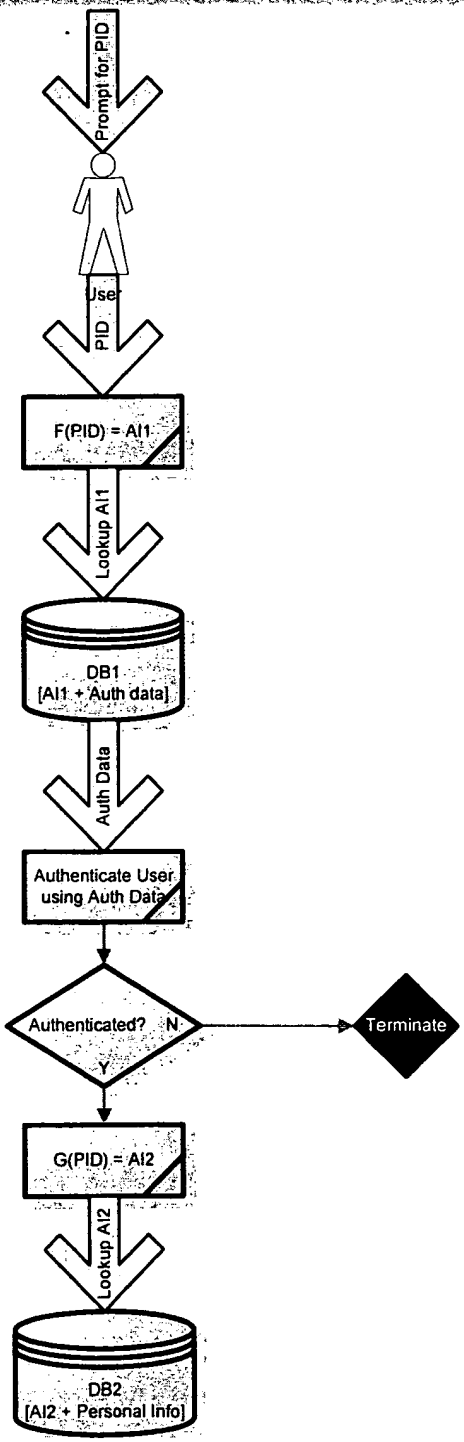
accessing data associated with the user stored in a first database using the first anonymous identifier;

authenticating the user using the data associated with the user accessed in said first database using the first anonymous identifier;

identifying a second anonymous identifier from information derived from the user's personal identifier if the step of authenticating is positive; and

using the second anonymous identifier to access personal information associated with the user stored in a second database.

80. A method for accessing personal information, associated with a plurality of users and stored in a computer system, in a manner that protects the privacy of users, wherein each user has a personal identifier and a plurality of anonymous identifiers, comprising the steps of:
80.1 prompting a user for the user's personal identifier;
80.2 determining a first anonymous identifier from information derived from the user's personal identifier;
80.3 accessing data associated with the user stored in a first database using the first anonymous identifier;
80.4 authenticating the user using the data associated with the user accessed in said first database using the first anonymous identifier;
80.5 determining a second anonymous identifier from information derived from the user's personal identifier if the step of authenticating is positive; and
80.6 using the second anonymous identifier to access personal information associated with the user stored in a second database.



Claim 81. The method for accessing personal information recited in claim 80, further comprising the steps of:

providing the user's personal identifier to a first server computer, said first server computer performing the step of determining the first anonymous identifier;

providing the first anonymous identifier to a second server computer, said second server computer performing the steps of accessing data from said first database and authenticating the user, said second server computer further providing a positive indication to the first server computer further providing a positive indication to the first server computer if the user is successfully authenticated;

wherein in said first server computer preforms the step of determining the second anonymous identifier in response to a positive indication from the second server computer further providing the second anonymous identifier to a third server computer, said third server computer performing the step of accessing personal information associated with the user from said second database.

81. The method for accessing personal information recited in claim 80, further comprising the steps of:
81.1 providing the user's personal identifier to a first server computer, said first server computer performing the step of determining the first anonymous identifier;
81.2 providing the first anonymous identifier to a second server computer, said second server computer performing the steps of accessing data from said first database and authenticating the User, said second server computer further providing a positive indication to the first server computer if the user is successfully authenticated;
81.3 wherein said first server computer performs the step of determining the second anonymous identifier in response to a positive indication from the second server computer, said first server computer further providing the second anonymous identifier to a third server computer, said third server computer performing the step of accessing personal information associated with the user from said second database.